REMARKS

Applicant thanks the Examiner for the thorough consideration given the present application. Claims 1-20 are currently being prosecuted. The Examiner is respectfully requested to reconsider his rejections in view of the amendments and remarks as set forth below.

Substitute Specification

Applicant is submitting herewith a substitute specification in order to improve the language. These changes are not substantive and are primarily directed to wording changes to improve the understandability of the language.

Drawings

Applicant is preparing a drawing correction to be filed in the near future which utilizes the same new language now utilized throughout the specification in order to have the drawings be consistent with the specification changes. No new matter will be entered in this Amendment.

Rejection Under 35 U.S.C. § 103

Claims 1-20 stand rejected under 35 U.S.C. § 103 as being obvious over Ji et al. (U.S. Patent No. 5,889,943), in view of Kandasamy et al. (U.S. Patent No. 5,513,314). This rejection is respectfully traversed.

The application provides a backup/recovery system and methodology to securely back up and reliably retrieve data in a computer system. The computer system has a data storage device, such as a hard disk, with data stored thereon, on which real-time data backup protection is required, in order to receive data from LAN/WAN afterwards without risk. When network data is arrived to the computer system, the detecting module determines whether the received data is coming from the behavior of downloading from the network or receiving electronic mails via Outlook Express, comprising HTTP pages, E-mails, downloading files and so forth. If so, the detecting module determines whether the predetermined file contains predetermined harmful data, such as .exe, .zip, and .com extension files If there is a predetermined harmful data contained therein, the backup/recovery system backs up data stored in the hard disk, and the interface implements a predetermined procedure thereafter, so that application layer can access the predetermined file safely.

The restore point created by the application contains the backup data and identification information to identify the backup data. Such identification information is useful restoring the computer system in the future.

However, the 5,889,943 patent discloses an apparatus and method for electronic mail virus detection and elimination. The apparatus for detecting and eliminating viruses which may be introduced by messages sent through a postal node of a network electronic mail system includes polling and retrieval modules in communication with the postal node to determine the presence of unscanned messages and to download data associated with them to a node for treatment by a virus analysis and treatment module. A method for

detecting and eliminating viruses introduced by an electronic mail system includes polling the postal node for unscanned messages, downloading the messages into a memory of a node, and performing virus detection and analysis at the node.

The 5,889,943 patent suggests the file that can contain viruses to be temporarily stored at the gateway node, prior to determining if it contains viruses. If a virus is detected, the patent allows the temporary file to be deleted or erased from the gateway node; or to be renamed and stored in a specified directory on the gateway node. If no viruses are detected, the file will be transmitted.

When a user downloads a file which contains undefined viruses, the 5,889,943 patent can't recognize the viruses. So the file will be transmitted, and the viruses will likely to destroy data stored in the hard disk. Moreover, if files in the operating system are infected and destroyed, the operating system, such as Windows, cannot be rebooted. The more serious effect is that the computer system needs to be setup again.

In case of a virus detected by the patent, the temporary file stored in a specified directory on the gateway node can not be used by any conventional backup/recovery software to restore the hard disk to a previous state. In other words, the 5,889,943 patent provides no notion of how to solve the problem of virus-infected hard disk, not to mention the reconstruction operation. This, however, makes the users at the risk of losing data in the hard disk.

In contrast, the application has the backup/recovery techniques to back up and/or recover data in the data storage device. A restore point can be created prior to downloading an executable file. In the event of virus attack and the computer system crash,

the backup/recovery system and methodology enables the user to instantly recover deleted or overwritten files, and the computer system configuration, to any point in time prior to the downloaded data arrival. The files and the system configuration are cleanly and completely restored in minutes. Hence, the improvement of the application is remarkable for the data storage device while its data is under whole automatic protection from viruses.

The 5,513,314 patent is not aware of data backup operation prior to receiving emails or downloading files or software from the Internet in any way. If a computer virus has crashed the computer system, the user can't restore back to the exact pre-infected state. Therefore, some of the files that exist before the user receives the virus-infected email or downloads the virus-infected files might be lost permanently.

Accordingly, the 5,889,943 patent and the 5,513,314 patent do not suggest or render obvious the application. Those skilled in the art will not realize that creating a restore point prior to downloading an executable file.

Accordingly, Applicant submits that claims 1-20 are patentable over this rejection.

Conclusion

In view of the above remarks, it is believed that the claims clearly distinguish over the patents relied on by the Examiner, either alone or in combination. In view of this, reconsideration of the rejections and allowance of all the claims are respectfully requested.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Robert F. Gnuse (Reg. No.

27,295) at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

Pursuant to 37 C.F.R. §§ 1.17 and 1.136(a), Applicants respectfully petition for a two (2) month extension of time for filing a response in connection with the present application and the required fee of $210 is being filed concurrently herewith.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By _____
Joe McKinney Muncy, #32,334

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

KM/RFG/ags
3667-0102P

Attachment(s): Substitute Specification
Abstract of the Disclosure

(Rev. 09/30/03)